APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/421,919	10/20/1999	PAUL L. JERAN	10990500-1	4776

22879	7590	11/17/2004

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
MAHMOUDI, HASSAN

ART UNIT	PAPER NUMBER
2165	

DATE MAILED: 11/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/421,919	JERAN, PAUL L.
	Examiner	Art Unit	
	Tony Mahmoudi	2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _22 June 2004_.
2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-35_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _1-35_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 22-June-2004, claims 1, 13, 21-23, 29-31,

and 33 have been amended per applicant's request. Claims 1-35 are presently

pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that said subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-5, 7-12, 17-18, 21-24, and 29-31 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Cohen (U.S. Patent No. 6,356,941 B1) in view of Rose (U.S.

Patent No. 6,314,500 B1.)

As to claim 1, Cohen teaches in a computer system including at least one client

computer coupled by a communications network (see figure 1) to a remote secure

storage facility (see "protected central storage facility" in Abstract) located remotely

to the client computer (see column 2, lines 56-60), a method of accessing a dedicated

data storage unit (see Abstract and see column 2, lines 65-67 for storing data files (see

column 4, lines 23-25) in a secure environment (see Abstract, and see column 13,

lines 42-51), the method comprising:

initiating a request for accessing a dedicated data storage unit of the remote secure

storage facility (see column 13, lines 36-43), the remote secure storage facility

associated with an address on the communications network (see column 11, lines 46-

65);

in response to the request (see column 13, lines 42-51), automatically connecting

to the remote secure storage facility at the associated address (see column 4, lines 37-

45);

transmitting the request to the remote secure storage facility (see column 14, lines

46-65, and see column 15, lines 17-28); and

granting access to the identified dedicated data storage unit (see column 9, lines

32-46.)

Cohen does not teach the data storage unit associated with a user identification

code;

the request specifying at least the remote secure storage facility and a user

identification code; and

identifying the dedicated data storage unit associated with the specified user

identification code.

Rose teaches a data processing system (see Abstract), in which he teaches:

the data storage unit associated with a user identification code (see Abstract; see

column 5, lines 4-9, and column 8, lines 25-36);

the request specifying at least the remote secure storage facility and a user

identification code (see Abstract; see column 3, lines 16-18, and column 5, lines 1-4);

and

identifying the dedicated data storage unit associated with the specified user

identification code (see column 3, lines 27-46, and see column 3, lines 53-64, and see

column 8, lines 37-59.)

Therefore, it would have been obvious to a person having ordinary skill in the art

to have modified Cohen to include: the data storage unit associated with a user

identification code; the request specifying at least the remote secure storage facility

and a user identification code; and identifying the dedicated data storage unit

associated with the specified user identification code.

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Cohen by the teachings of Rose, because

including the data storage unit associated with a user identification code; the request

specifying at least the remote secure storage facility and a user identification code;

and identifying the dedicated data storage unit associated with the specified user

identification code, would enable the system to store and retrieve data to/from

specific dedicated portions of secured data storage devices, based on the user

identification and the identification of the data source. This inclusion allows selective

routing of data to different memory sources in a shared memory system. This

permits, for example, data to be routed to only a portion of the memory sources

associated with a given requester, thereby reducing the bandwidth to other memory

sources and reducing overall latencies within the system, as taught by Rose (see

column 3, lines 10-20.)

As to claim 2, <u>Cohen</u> as modified teaches wherein the step of granting access includes granting access to the identified dedicated storage unit (see <u>Cohen</u>, column 9, lines 1-22) in accordance with pre-existing instructions associated with the specified user identification code (see <u>Rose</u>, column 3, lines 39-47, and see column 8, line 60 through column 9, line 5.)

As to claim 3, <u>Cohen</u> as modified teaches wherein the request further specifies a processor identification code associated with a client computer, the step of identifying the dedicated data storage unit including identifying the dedicated data storage unit associated with both the specified user identification code and the specified processor identification code (see <u>Rose</u>, column 3, lines 39-47; column 4, lines 45-60, and see column 9, lines 29-31.)

As to claim 4, <u>Cohen</u> as modified teaches the method including the further step of displaying to a user a directory of data files stored in the dedicated data storage unit (see <u>Cohen</u>, column 10, lines 49-59.)

As to claim 5, <u>Cohen</u> as modified teaches the method including the further steps of:

selecting a data file from the displayed directory of data files (see <u>Cohen</u>, column 9, line 66 through column 10, line 19, and see column 10, lines 46-52); and

transmitting the selected data file to a client computer associated with the request

(see Cohen, column 5, lines 16-18; column 10, lines 52-59, and see column 12, lines

25-38.)

As to claim 7, Cohen as modified teaches wherein the request further specifies at

least one data file stored on the identified dedicated data storage unit (see Cohen,

column 3, lines 53-64), the method further comprising the step of transmitting the

specified at least one data file to a client computer associated with the request (see

Cohen, column 5, lines 16-18; column 10, lines 52-59, and see column 12, lines 25-

38.)

As to claims 8 and 9, Cohen as modified teaches each data file stored in the

dedicated data storage unit (see Cohen, Abstract) is assigned a reference identification

number by the secure storage facility at the time each data file is initially stored in the

dedicated data storage unit (see Rose, column 8, lines 56-59, and see column 9, lines

61-65.)

As to claim 10, Cohen as modified teaches the method including the further steps

of:

storing one or more data files in the dedicated data storage unit after access has

been granted (see Cohen, column 2, lines 53-56, and see column 5, lines 40-57); and

encrypting the data in the one or more data files in accordance with a user

assigned security level associated with each data file to be stored (see Cohen, column

12, lines 38-42.)

As to claim 11, Cohen as modified teaches wherein the step of encrypting the data

includes the step of encrypting the data at the secure storage facility prior to storing

the one or more data files in the dedicated data storage unit (see Cohen, column 12,

lines 35-38, and see column 17, lines 62-65.)

As to claim 12, Cohen as modified teaches wherein the step of encrypting the data

includes the step of encrypting the data at a client computer associated with the

request prior to storing the one or more data files in the dedicated data storage unit

(see Cohen, column 15, lines 24-28.)

As to claim 17, Cohen teaches a secure storage facility having an address on a

communications network (see column 11, lines 46-65) and adapted for

communication with other devices on the communications network (see column 12,

lines 24-43.)

For the remaining steps of this claim, applicant is kindly directed to remarks and

discussions made in claim 1 above.

As to claim 18, Cohen as modified teaches the facility further comprising

encryption and decryption means for encrypting and decrypting data files associated

with a user identification code in accordance with the set of instructions associated

with the user identification code (see Cohen, column 12, lines 39-43.)

As to claim 21, Cohen teaches a secure data storage system (see Abstract),

comprising:

a communications network address configured to identify the secure data storage

system to a remote computing device communicatively coupled to the secure data

storage system via the communications network (see column 4, lines 23-45);

a dedicated data storage unit configured to maintain data files generated by the

remote computing device (see column 17, lines 1-7); and

a processing component (see column 4, lines 46-60) configured to receive and

process a request to access the dedicated data storage unit (see column 5, lines 4-15),

the request specifying the communications network address, the identification code,

and a data file maintained with the dedicated data storage unit (see column 11, lines

46-65.)

For the teaching of "the dedicated data storage unit identified by an identification

code corresponding to the remote computing device", the applicant is directed to the

remarks and discussions made in claim 1 above.

As to claims 22 and 30, Cohen as modified teaches wherein the identification

code includes a processor identification code corresponding to the remote computing

device (see Rose, column 3, lines 39-47.)

As to claims 23 and 31, <u>Cohen</u> as modified teaches wherein the identification code includes a user identification code and a processor identification code corresponding to the remote computing device (see <u>Rose</u>, column 5, lines 1-9.)

As to claim 24, <u>Cohen</u> as modified teaches wherein the processing component is further configured to grant access to the dedicated data storage unit in accordance with access instructions associated with the identification code (see <u>Rose</u>, column 3, lines 39-47.)

As to claim 29, <u>Cohen</u> teaches a method (see column 1, lines 5-10), comprising:

maintaining data files (see column 10, lines 20-25) with a dedicated data storage unit (see column 17, lines 1-7), the dedicated data storage unit having an associated communications network address (see column 11, lines 46-65);

receiving a request to access the dedicated data storage unit the request specifying the communications network address, and a data file maintained with the dedicated data storage unit (see column 13, lines 31-51); and

granting access for the remote computing device to access the dedicated data storage unit in accordance with access instructions (see column 11, lines 24-32.)

for the teaching of "dedicated data storage unit that is identified by an identification code corresponding to a computing device", the applicant is directed to the remarks and discussions made in claim 1 above.

4. Claims 6, 19-20, 25, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cohen (U.S. Patent No. 6,356,941 B1) in view of Rose (U.S. Patent No.

6,314,500 B1), as applied to claims 1-5, 7-12, 17-18, 21-24, and 29-31 above, and

further in view of Mooney et al (U.S. Patent No. 6,351,813 B1.)

As to claims 6 and 19, Cohen as modified teaches wherein each data file is stored

in the dedicated data storage unit, each data file being encrypted (see Cohen, column

17, lines 62-65.)

Cohen as modified still does not teach wherein each data file has a predetermined

security level assigned thereto, each data file being encrypted in accordance with its

assigned security level.

Mooney et al teaches an access control/crypto system (see Abstract), in which he

teaches wherein each data file has a predetermined security level assigned thereto (see

figure 9, and see column 5, lines 16-41, and column 14, lines 63-66), each data file

being encrypted in accordance with its assigned security level (see column 17, lines

22-28.)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to have modified Cohen as modified, to include

wherein each data file has a predetermined security level assigned thereto, each data

file being encrypted in accordance with its assigned security level.

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Cohen as modified, by the teaching of

Mooney et al, because wherein each data file has a predetermined security level

assigned thereto, each data file being encrypted in accordance with its assigned

security level, enhances the data security by supporting multiple levels of security

based on various predetermined user criteria. Assigning a security level to each data

file provides a measure of the number of hierarchical steps required to be completed

before the user can have access to the file, as taught by Mooney et al (see column 5,

lines 16-18.)

As to claim 20, Cohen as modified teaches wherein the set of instructions

associated with a user identification code (see Rose, column 3, lines 39-47) specifies

read-only, write only or read/write access to data files stored in the dedicated data

storage unit associated with that user identification code (see Mooney et al, column

15, lines 1-4.)

As to claims 25 and 32, Cohen as modified teaches wherein the processing

component is further configured to encrypt the data files in accordance with a security

level (see Mooney et al, column 15, lines 1-4) associated with the identification code

(see Rose, column 3, lines 39-47.)

5.   Claims 13-14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cohen (U.S. Patent No. 6,356,941 B1) in view of Rose (U.S. Patent No. 6,314,500

B1), as applied to claims 1-5, 7-12, 17-18, 21-24, and 29-31 above, and further in

view of Weber (U.S. Patent No. 6,067,618.)

As to claim 13, <u>Cohen</u> teaches in a computer system including at least one client computer coupled by a communications network to a secure storage facility located remotely to the client computer, the remote secure storage facility identified by an address on the communications network and including at least one dedicated data storage unit for storing data files associated with a user identification code in a secure environment, encryption /decryption means and processor means, the remote secure storage facility adapted to allow access to the at least one dedicated data storage unit in accordance with a set of pre-existing instructions, apparatus for accessing the at least one dedicated data storage unit such that the remote secure storage facility is transparent to a client computer (for these and remaining steps of this claim, applicant is kindly directed to the remarks and discussions for modifying <u>Cohen</u> with the teachings of <u>Rose</u>, made in claims 1-5, 7, and 10-12 above.)

<u>Cohen</u> as modified does not teach: a logical data storage peripheral coupled to a client computer, the logical data storage peripheral associated with a remote secure storage facility; and

a controller associated with the logical data storage peripheral and storing the address on the communications network of at least one remote secure storage facility.

<u>Weber</u> teaches a user storage separation system (see Abstract), in which he teaches:

a logical data storage peripheral coupled to the client computer, the logical data storage peripheral associated with the remote secure storage facility (see column 9, lines 41-65, and see column 17, line 65 through column 18, line 4); and

a controller associated with the logical data storage peripheral and storing the address on the communications network of the remote secure storage facility (see column 18, lines 5-20.)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Cohen as modified, to include a logical data storage peripheral coupled to a client computer, the logical data storage peripheral associated with a remote secure storage facility; and a controller associated with the logical data storage peripheral and storing the address on the communications network of at least one remote secure storage facility.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Cohen as modified, by the teaching of Weber, because including a logical data storage peripheral coupled to a client computer, the logical data storage peripheral associated with a remote secure storage facility; and a controller associated with the logical data storage peripheral and storing the address on the communications network of at least one remote secure storage facility, would provide portability and more control to the user, such as enabling the user to load software programs and store portable files, as taught by Weber (see column 18, lines 9-10.)

As to claim 14, Cohen as modified teaches the apparatus further comprising encryption and decryption means for encrypting data files to be stored in a dedicated data storage unit and decrypting data files retrieved from a dedicated data storage unit (see Cohen, column 12, lines 39-43.)

As to claim 16, Cohen as modified teaches the apparatus further comprising

memory means for storing at least one directory, each directory containing a listing of

data files stored in a dedicated data storage unit (see Cohen, column 10, lines 52-59.)

6. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen (U.S.

Patent No. 6,356,941 B1) in view of Rose (U.S. Patent No. 6,314,500 B1), and

further in view of Weber (U.S. Patent No. 6,067,618), as applied to claims 13-14 and

16 above, and still further in view of Mooney et al (U.S. Patent No. 6,351,813 B1.)

As to claim 15, Cohen as modified teaches wherein a data file to be stored in the

dedicated data storage unit associated with a user identification code (see Rose,

column 3, lines 39-47.)

Cohen as modified still does not teach encrypting in accordance with a user

assigned security level.

Mooney et al teaches an access control/crypto system (see Abstract), in which he

teaches encrypting in accordance with its assigned security level (see column 15,

lines 1-4, and see column 17, lines 22-28.)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to have modified Cohen as modified, to include

encrypting in accordance with its assigned security level.

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Cohen as modified, by the teaching of

Mooney et al, because encrypting in accordance with its assigned security level

would provide assigning a security level to each data file provides a measure of the

number of hierarchical steps required to be completed before the user can have access

to the file, as taught by Mooney et al (see column 5, lines 16-18.)

7. Claims 26-28 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Allen et al (U.S. Patent No. 5,546,557) in view of Rose (U.S. Patent No.

6,314,500 B1.)

As to claim 26, Allen et al teaches a computing device (see column 9, lines 9-16),

comprising:

a logical data storage peripheral (see Abstract and see figure 2, and column 9,

lines 34-36) corresponding to a remote secure data storage system that includes a

dedicated data storage unit configured to maintain data files generated by the

computing device (see Abstract, see figure 12, and see and see column 8, lines 42-

45);

a controller configured to receive a request to access the logical data storage

peripheral (see column 14, lines 45-50), the request specifying the logical data storage

peripheral, and a data file maintained with the dedicated data storage unit (see column

22, lines 21-26); and

the controller further configured to communicatively couple the computing device

to the remote secure data storage system and communicate the request to access the

logical data storage peripheral to the remote secure data storage system (see column

27, lines 62-65, and see column 28, lines 59-61, and see column 30, lines 41-67.)

Allen et al does not teach the dedicated data storage unit identified by an

identification code corresponding to the computing device.

Rose teaches a data processing system (see Abstract), in which he teaches:

the dedicated data storage unit identified by an identification code corresponding

to the computing device (see column 3, lines 39-64.)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to have modified Allen et al to include the

dedicated data storage unit identified by an identification code corresponding to the

computing device.

It would have been obvious to a person having ordinary skill in the art at the time

the invention was made to have modified Allen et al by the teaching of Rose, because

including the dedicated data storage unit identified by an identification code

corresponding to the computing device, would enable the system to access the

appropriate (requested) storage device associated with the user/data for storage and

retrieval purposes.

As to claims 27 and 34, Allen et al as modified teaches the device further

comprising a processor configured to execute the controller, and wherein the

identification code includes a processor identification code corresponding to the

computing device (see Rose, column3, lines 39-47.)

As to claims 28 and 35, Allen et al as modified teaches the device further comprising a processor configured to execute the controller (see Allen et al, Abstract, and see column 7, lines 25-42) , and wherein the identification code includes a user identification code and a processor identification code corresponding to the computing device (see Rose, column 3, lines 39-47).

As to claim 33, the applicant is directed to the remarks and discussions made in claim 26 above.

Response to Arguments

8. Applicant's arguments filed on 22-June-2004 with respect to the rejected claims in view of the cited references have been fully considered but they are not deemed persuasive:

In response the applicant's arguments that there is no motivation to combine Rose with Cohen, the arguments have been fully considered but are not deemed persuasive, because the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both cited references teach inventions that are in the same field of endeavor, and the

combination would cause data to be routed to only a portion of the memory sources

associated with a given requester, thereby reducing the bandwidth to other memory

sources and reducing overall latencies within the system, as taught by Rose (see

column 3, lines 10-20.)

In response to the applicant's arguments that "there is no indication whatsoever in

Rose of a remote data storage connected via a network to a computer", the arguments

have been fully considered but are not deemed persuasive, because Rose teaches "the

operational logic for implementing selective data routing consistent with the

invention is typically distributed among the various sources and response

combination logic" (see column 9, lines 32-41.) Further, Rose teaches "System 10

generically represents, for example, any of a number of multi-user computer systems

such as a network server, a midrange computer, a mainframe computer, etc." (see

column 5, lines 10-25.)

In response to the applicant's arguments that "Cohen and/or Rose do not show or

disclose a request specifying a remote secure storage facility and a user identification

code", the arguments have been fully considered but are not deemed persuasive,

because Cohen teaches initiating a request for accessing a dedicated data storage unit

(see column 13, lines 36-43), and he teaches "remote" storage facility in "the network

vault can be accessed through a network from a remote location, such that the user

does not necessarily need to be in the same physical location as the central storage

facility in order to place data into, and retrieve data from, the network vault." (see

column 2, lines 56-65.) <u>Rose</u> teaches "the data storage unit associated with a user

identification code" (see Abstract; see column 5, lines 4-9, and column 8, lines 25-

36.) With respect to <u>Rose</u> not being "analogous", the applicant is directed to the

remarks and discussions made above.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed

within TWO MONTHS of the mailing date of this final action and the advisory action

is not mailed until after the end of the THREE-MONTH shortened statutory period,

then the shortened statutory period will expire on the date the advisory action is

mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from

the mailing date of the advisory action. In no event, however, will the statutory

period for reply expire later than SIX MONTHS from the mailing date of this final

action.

10. Any inquiries concerning this communication or earlier communications from the

examiner should be directed to Tony Mahmoudi whose telephone number is (571)

272-4078. The examiner can normally be reached on Mondays-Fridays from 08:00

am to 04:30 pm.

     If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Dov Popovici, can be reached at (571) 272-4083.

tm

November 9, 2004

SAM RIMELL
PRIMARY EXAMINER